

JS 44 (Rev. 02/19)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. (SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)

I. (a) PLAINTIFFS

KELLY EMERY

(b) County of Residence of First Listed Plaintiff Bucks
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys (Firm Name, Address, and Telephone Number)
Gary F. Lynch, Carlson Lynch LLP
1133 Penn Avenue, 5th Floor
Pittsburgh, PA 15222 (412) 322-9243

DEFENDANTS

WAWA, INC. and WILD GOOSE HOLDING CO., INC.

County of Residence of First Listed Defendant Delaware
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys (If Known)

II. BASIS OF JURISDICTION (Place an "X" in One Box Only)

- ☐ 1 U.S. Government Plaintiff
☐ 2 U.S. Government Defendant
☐ 3 Federal Question (U.S. Government Not a Party)
☒ 4 Diversity (Indicate Citizenship of Parties in Item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (Place an "X" in One Box for Plaintiff and One Box for Defendant)

- | PTF | DEF | PTF | DEF |
|---|---|----------------------------|---------------------------------------|
| <input checked="" type="checkbox"/> 1 | <input type="checkbox"/> 1 | <input type="checkbox"/> 4 | <input checked="" type="checkbox"/> 4 |
| Citizen of This State | Incorporated or Principal Place of Business In This State | | |
| <input type="checkbox"/> 2 | <input type="checkbox"/> 2 | <input type="checkbox"/> 5 | <input type="checkbox"/> 5 |
| Citizen of Another State | Incorporated and Principal Place of Business In Another State | | |
| <input type="checkbox"/> 3 | <input type="checkbox"/> 3 | <input type="checkbox"/> 6 | <input type="checkbox"/> 6 |
| Citizen or Subject of a Foreign Country | Foreign Nation | | |

IV. NATURE OF SUIT (Place an "X" in One Box Only)

Click here for: Nature of Suit Code Descriptions.

<input type="checkbox"/> 110 Insurance <input type="checkbox"/> 120 Marine <input type="checkbox"/> 130 Miller Act <input type="checkbox"/> 140 Negotiable Instrument <input type="checkbox"/> 150 Recovery of Overpayment & Enforcement of Judgment <input type="checkbox"/> 151 Medicare Act <input type="checkbox"/> 152 Recovery of Defaulted Student Loans (Excludes Veterans) <input type="checkbox"/> 153 Recovery of Overpayment of Veteran's Benefits <input type="checkbox"/> 160 Stockholders' Suits <input type="checkbox"/> 190 Other Contract <input type="checkbox"/> 195 Contract Product Liability <input type="checkbox"/> 196 Franchise	PERSONAL INJURY <input type="checkbox"/> 310 Airplane <input type="checkbox"/> 315 Airplane Product Liability <input type="checkbox"/> 320 Assault, Libel & Slander <input type="checkbox"/> 330 Federal Employers' Liability <input type="checkbox"/> 340 Marine <input type="checkbox"/> 345 Marine Product Liability <input type="checkbox"/> 350 Motor Vehicle <input type="checkbox"/> 355 Motor Vehicle Product Liability <input checked="" type="checkbox"/> 360 Other Personal Injury <input type="checkbox"/> 362 Personal Injury - Medical Malpractice	PERSONAL INJURY <input type="checkbox"/> 365 Personal Injury - Product Liability <input type="checkbox"/> 367 Health Care/Pharmaceutical Personal Injury Product Liability <input type="checkbox"/> 368 Asbestos Personal Injury Product Liability PERSONAL PROPERTY <input type="checkbox"/> 370 Other Fraud <input type="checkbox"/> 371 Truth in Lending <input type="checkbox"/> 380 Other Personal Property Damage <input type="checkbox"/> 385 Property Damage Product Liability	<input type="checkbox"/> 625 Drug Related Seizure of Property 21 USC 881 <input type="checkbox"/> 690 Other	<input type="checkbox"/> 422 Appeal 28 USC 158 <input type="checkbox"/> 423 Withdrawal 28 USC 157 <input type="checkbox"/> 820 Copyrights <input type="checkbox"/> 830 Patent <input type="checkbox"/> 835 Patent - Abbreviated New Drug Application <input type="checkbox"/> 840 Trademark	<input type="checkbox"/> 375 False Claims Act <input type="checkbox"/> 376 Qui Tam (31 USC 3729(a)) <input type="checkbox"/> 400 State Reapportionment <input type="checkbox"/> 410 Antitrust <input type="checkbox"/> 430 Banks and Banking <input type="checkbox"/> 450 Commerce <input type="checkbox"/> 460 Deportation <input type="checkbox"/> 470 Racketeer Influenced and Corrupt Organizations <input type="checkbox"/> 480 Consumer Credit <input type="checkbox"/> 485 Telephone Consumer Protection Act <input type="checkbox"/> 490 Cable/Sat TV <input type="checkbox"/> 850 Securities/Commodities/Exchange <input type="checkbox"/> 890 Other Statutory Actions <input type="checkbox"/> 891 Agricultural Acts <input type="checkbox"/> 893 Environmental Matters <input type="checkbox"/> 895 Freedom of Information Act <input type="checkbox"/> 896 Arbitration <input type="checkbox"/> 899 Administrative Procedure Act/Review or Appeal of Agency Decision <input type="checkbox"/> 950 Constitutionality of State Statutes
<input type="checkbox"/> 210 Land Condemnation <input type="checkbox"/> 220 Foreclosure <input type="checkbox"/> 230 Rent Lease & Ejectment <input type="checkbox"/> 240 Torts to Land <input type="checkbox"/> 245 Tort Product Liability <input type="checkbox"/> 290 All Other Real Property	<input type="checkbox"/> 440 Other Civil Rights <input type="checkbox"/> 441 Voting <input type="checkbox"/> 442 Employment <input type="checkbox"/> 443 Housing/Accommodations <input type="checkbox"/> 445 Amer. w/Disabilities - Employment <input type="checkbox"/> 446 Amer. w/Disabilities - Other <input type="checkbox"/> 448 Education	Habeas Corpus: <input type="checkbox"/> 463 Alien Detainee <input type="checkbox"/> 510 Motions to Vacate Sentence <input type="checkbox"/> 530 General <input type="checkbox"/> 535 Death Penalty Other: <input type="checkbox"/> 540 Mandamus & Other <input type="checkbox"/> 550 Civil Rights <input type="checkbox"/> 555 Prison Condition <input type="checkbox"/> 560 Civil Detainee - Conditions of Confinement	<input type="checkbox"/> 710 Fair Labor Standards Act <input type="checkbox"/> 720 Labor/Management Relations <input type="checkbox"/> 740 Railway Labor Act <input type="checkbox"/> 751 Family and Medical Leave Act <input type="checkbox"/> 790 Other Labor Litigation <input type="checkbox"/> 791 Employee Retirement Income Security Act	<input type="checkbox"/> 861 HIA (1395ff) <input type="checkbox"/> 862 Black Lung (923) <input type="checkbox"/> 863 DIWC/DIWW (405(g)) <input type="checkbox"/> 864 SSID Title XVI <input type="checkbox"/> 865 RSI (405(g))	
			<input type="checkbox"/> 462 Naturalization Application <input type="checkbox"/> 465 Other Immigration Actions	<input type="checkbox"/> 870 Taxes (U.S. Plaintiff or Defendant) <input type="checkbox"/> 871 IRS—Third Party 26 USC 7609	

V. ORIGIN (Place an "X" in One Box Only)

- ☒ 1 Original Proceeding
☐ 2 Removed from State Court
☐ 3 Remanded from Appellate Court
☐ 4 Reinstated or Reopened
☐ 5 Transferred from Another District (specify)
☐ 6 Multidistrict Litigation - Transfer
☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing (Do not cite jurisdictional statutes unless diversity):
Class Action Fairness Act ("CAFA", 28 U.S.C. § 1332(d))

Brief description of cause:
Defendants' negligence led to security breach compromising Plaintiff's data

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A CLASS ACTION UNDER RULE 23, F.R.Cv.P.

DEMAND \$

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions):

JUDGE

DOCKET NUMBER

DATE
12/23/2019

SIGNATURE OF ATTORNEY OF RECORD

FOR OFFICE USE ONLY

RECEIPT #

AMOUNT

APPLYING IFP

JUDGE

MAG. JUDGE

DEC 23 2019

UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

DESIGNATION FORM

(to be used by counsel or pro se plaintiff to indicate the category of the case for the purpose of assignment to the appropriate calendar)

Address of Plaintiff: 1828 Willow Avenue, Bristol, PA 19007

Address of Defendant: Wawa, Inc. and Wild Goose Holding Co., Inc., 260 W. Baltimore Pike, Wawa, PA 19063

Place of Accident, Incident or Transaction: Various

RELATED CASE, IF ANY:

Case Number: _____ Judge: _____ Date Terminated: _____

Civil cases are deemed related when Yes is answered to any of the following questions:

- | | | |
|--|------------------------------|--|
| 1. Is this case related to property included in an earlier numbered suit pending or within one year previously terminated action in this court? | Yes <input type="checkbox"/> | No <input checked="" type="checkbox"/> |
| 2. Does this case involve the same issue of fact or grow out of the same transaction as a prior suit pending or within one year previously terminated action in this court? | Yes <input type="checkbox"/> | No <input checked="" type="checkbox"/> |
| 3. Does this case involve the validity or infringement of a patent already in suit or any earlier numbered case pending or within one year previously terminated action of this court? | Yes <input type="checkbox"/> | No <input checked="" type="checkbox"/> |
| 4. Is this case a second or successive habeas corpus, social security appeal, or pro se civil rights case filed by the same individual? | Yes <input type="checkbox"/> | No <input checked="" type="checkbox"/> |

I certify that, to my knowledge, the within case ☐ is ☒ is not related to any case now pending or within one year previously terminated action in this court except as noted above.

DATE: 12/23/2019

[Signature]
Attorney-at-Law / Pro Se Plaintiff

56887

Attorney I.D. # (if applicable)

CIVIL: (Place a ✓ in one category only)

A. Federal Question Cases:

- ☐ 1. Indemnity Contract, Marine Contract, and All Other Contracts
 - ☐ 2. FELA
 - ☐ 3. Jones Act-Personal Injury
 - ☐ 4. Antitrust
 - ☐ 5. Patent
 - ☐ 6. Labor-Management Relations
 - ☐ 7. Civil Rights
 - ☐ 8. Habeas Corpus
 - ☐ 9. Securities Act(s) Cases
 - ☐ 10. Social Security Review Cases
 - ☐ 11. All other Federal Question Cases
- (Please specify): _____

B. Diversity Jurisdiction Cases:

- ☐ 1. Insurance Contract and Other Contracts
 - ☐ 2. Airplane Personal Injury
 - ☐ 3. Assault, Defamation
 - ☐ 4. Marine Personal Injury
 - ☐ 5. Motor Vehicle Personal Injury
 - ☐ 6. Other Personal Injury (Please specify): _____
 - ☐ 7. Products Liability
 - ☐ 8. Products Liability - Asbestos
 - ☒ 9. All other Diversity Cases
- (Please specify): Class Action Fairness Act, 28 USC 1332(d)

ARBITRATION CERTIFICATION

(The effect of this certification is to remove the case from eligibility for arbitration.)

I, Gary F. Lynch, counsel of record or pro se plaintiff, do hereby certify:



Pursuant to Local Civil Rule 53.2, § 3(c) (2), that to the best of my knowledge and belief, the damages recoverable in this civil action case exceed the sum of \$150,000.00 exclusive of interest and costs:



Relief other than monetary damages is sought.

DATE: 12/23/2019

[Signature]
Attorney-at-Law / Pro Se Plaintiff

56887

Attorney I.D. # (if applicable)

NOTE: A trial de novo will be a trial by jury only if there has been compliance with F.R.C.P. 38.

DEC 23 2019

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

CASE MANAGEMENT TRACK DESIGNATION FORM

KELLY EMERY, on behalf of herself and all
others similarly situated,

CIVIL ACTION

v.

WAWA, INC. and WILD GOOSE
HOLDING CO., INC.

19 NO. 6077

In accordance with the Civil Justice Expense and Delay Reduction Plan of this court, counsel for plaintiff shall complete a Case Management Track Designation Form in all civil cases at the time of filing the complaint and serve a copy on all defendants. (See § 1:03 of the plan set forth on the reverse side of this form.) In the event that a defendant does not agree with the plaintiff regarding said designation, that defendant shall, with its first appearance, submit to the clerk of court and serve on the plaintiff and all other parties, a Case Management Track Designation Form specifying the track to which that defendant believes the case should be assigned.

SELECT ONE OF THE FOLLOWING CASE MANAGEMENT TRACKS:

- (a) Habeas Corpus – Cases brought under 28 U.S.C. § 2241 through § 2255. ()
- (b) Social Security – Cases requesting review of a decision of the Secretary of Health and Human Services denying plaintiff Social Security Benefits. ()
- (c) Arbitration – Cases required to be designated for arbitration under Local Civil Rule 53.2. ()
- (d) Asbestos – Cases involving claims for personal injury or property damage from exposure to asbestos. ()
- (e) Special Management – Cases that do not fall into tracks (a) through (d) that are commonly referred to as complex and that need special or intense management by the court. (See reverse side of this form for a detailed explanation of special management cases.) (X)
- (f) Standard Management – Cases that do not fall into any one of the other tracks. ()

12/23/2019

Date

412-322-9243

Telephone

G. Lynch
Attorney-at-law

412-231-0246

FAX Number

Plaintiff

Attorney for

glynch@carlsonlynch.com

E-Mail Address

DEC 23 2019

\$400

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF PENNSYLVANIA**

**KELLY EMERY, on behalf of herself and
all others similarly situated,**

Plaintiff,

v.

**WAWA, INC. and WILD GOOSE
HOLDING CO., INC.,**

Defendants.

Case No.

19 6077

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiff Kelly Emery ("Plaintiff"), on behalf of herself and all others similarly situated, asserts the following against Defendants WaWa, Inc. and Wild Goose Holding Co., Inc. (collectively, "WaWa" or "Defendants"), based upon personal knowledge, where applicable, information and belief, and the investigation of counsel.

I. INTRODUCTION

1. Plaintiff brings this class action on behalf of individual consumers against WaWa for its conscious failure to take adequate and reasonable measures to protect its point-of-sale payment terminals, fuel dispensers, and payment processing servers. WaWa's actions left its customers' highly sensitive payment card data, including, but not limited to, the cardholder name, credit or debit card number, and expiration date ("Payment Card Data") exposed and accessible for use by hackers from at least March 4, 2019 through December 12, 2019, at which time WaWa claims the breach was contained (the "WaWa Data Breach").

2. In or about March 2019, computer hackers accessed WaWa's inadequately protected point-of-sale systems and installed malicious software (often referred to as "malware") that infected potentially every WaWa in-store payment terminal and fuel dispenser in the United

States.¹ Through this malware, hackers stole the Payment Card Data of an untold number of customers.

3. The data breach was the inevitable result of WaWa's inadequate data security measures and lackadaisical approach to the security of its customers' Payment Card Data. Despite the well-publicized and ever-growing threat of cyber-attacks targeting Payment Card Data through vulnerable point-of-sale systems and inadequately protected computer networks, WaWa refused to implement certain best practices, failed to upgrade critical security systems, used outdated point-of-sale systems, ignored warnings about the vulnerability of its computer network, and disregarded and/or violated applicable industry standards.

4. WaWa's data security deficiencies were further buttressed by its failure to timely identify the breach and subsequently contain it. By December 19, 2019, when WaWa first publicly acknowledged that a data breach compromising customer Payment Card Data had occurred, the data breach already had been ongoing for several months. The malware had remained undetected within WaWa's point-of-sale and computer systems from at least March 2019 until December 10, 2019, when WaWa claims it first learned of the malware on its payment processing servers.

5. The financial costs and injuries to Plaintiff and other consumers caused by WaWa's deficient data security approach have been and will be significant, including:

- a. unauthorized charges on their debit and credit card accounts;
- b. theft of their personal and financial information;

¹ Wawa, WaWa Notifies Customers of Data Security Incident, https://s3.amazonaws.com/wawa-kentico-prod/wawa/media/misc/wawa-data-security-incident-wire-release-12_19_2019.pdf (Dec. 19, 2019) (last accessed Dec. 23, 2019).

- c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;
- d. damages arising from the inability to use their debit or credit card accounts because their accounts were suspended or otherwise rendered unusable as a result of fraudulent charges stemming from the WaWa Data Breach, including but not limited to foregoing cash back rewards;
- e. loss of use of and access to their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, lost opportunities to purchase gifts at discounted prices during the 2019 holiday shopping season, and adverse effects on their credit including decreased credit scores and adverse credit notations;
- f. costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the WaWa Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the stress, nuisance and annoyance of dealing with all issues resulting from the WaWa Data Breach;
- g. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their credit card and personal information

being placed in the hands of criminals and the risk of misuse via the sale of Plaintiff's and Class members' information on the Internet black market;

- h. money paid for products and services purchased at WaWa locations during the period of the WaWa Data Breach, in that Plaintiff and Class members would not have shopped at WaWa had WaWa disclosed that it lacked adequate systems and procedures to reasonably safeguard customers' Payment Card Data;
- i. damages to and diminution in value of their Payment Card Data entrusted to WaWa for the sole purpose of purchasing products and services from WaWa; and
- j. the loss of Plaintiff's and Class members' privacy.

6. This class action is brought on behalf of consumers throughout the U.S. to recover the damages they and others similarly situated have suffered, and continue to suffer, as a direct result of the WaWa Data Breach. Plaintiff asserts claims for negligence, negligence *per se*, and declaratory and injunctive relief.

II. PARTIES

A. Plaintiff

7. Plaintiff resides in and is a citizen of the Commonwealth of Pennsylvania.

B. Defendants

8. Defendant WaWa, Inc. is a privately-held New Jersey corporation with its principal place of business in WaWa, Pennsylvania. It is a citizen of Pennsylvania.

9. Defendant Wild Goose Holding Co., Inc. is a Delaware corporation. Its principal place of business is also in WaWa, Pennsylvania and it too is a Pennsylvania citizen. Defendant Wild Goose Holding Co., Inc. is WaWa, Inc.'s parent company.

10. WaWa is engaged in the business of developing and operating a system of convenience stores. WaWa currently operates more than 850 retail stores throughout Pennsylvania, New Jersey, Delaware, Maryland, Virginia, Florida, and Washington, D.C. WaWa offers gasoline at over 600 of these locations.² According to Forbes magazine, WaWa ranked 25th on the list of largest private companies in 2019, with a total revenue of \$12.1 billion.³

11. WaWa is not a franchisor. It has total control over the manner in which its more than 850 locations operate, including those locations' computer software and electronic data transmission systems for point of sale reporting.

III. JURISDICTION AND VENUE

12. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. §1332(d), because at least one Class member is of diverse citizenship from one defendant, there are more than 100 Class members, and the aggregate amount in controversy exceeds \$5 million, exclusive of interest and costs.

13. The Eastern District of Pennsylvania has personal jurisdiction over Defendants named in this action because Defendants are headquartered in Pennsylvania and conduct substantial business in Pennsylvania and this District through its headquarters, convenience stores, gas stations, and commercial website.

² WaWa, About WaWa, <https://www.wawa.com/about> (last accessed Dec. 23, 2019).

³ Forbes, #25 WaWa, <https://www.forbes.com/companies/wawa/#35178b652644> (last accessed Dec, 20, 2019).

14. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendants are headquartered in this District and have caused harm to Plaintiff and Class members residing in this District.

IV. FACTUAL ALLEGATIONS

A. Payment Card Processing Background

15. It is well known that customer Payment Card Data is valuable and often targeted by hackers. Over the last several years, numerous data breaches have occurred at large retailers and restaurants nationwide, including Wendy's, The Home Depot, Target, Kmart, P.F. Chang's, and many others. Despite widespread publicity and industry alerts regarding these other notable data breaches, WaWa failed to take reasonable steps to adequately protect its computer systems from being breached.

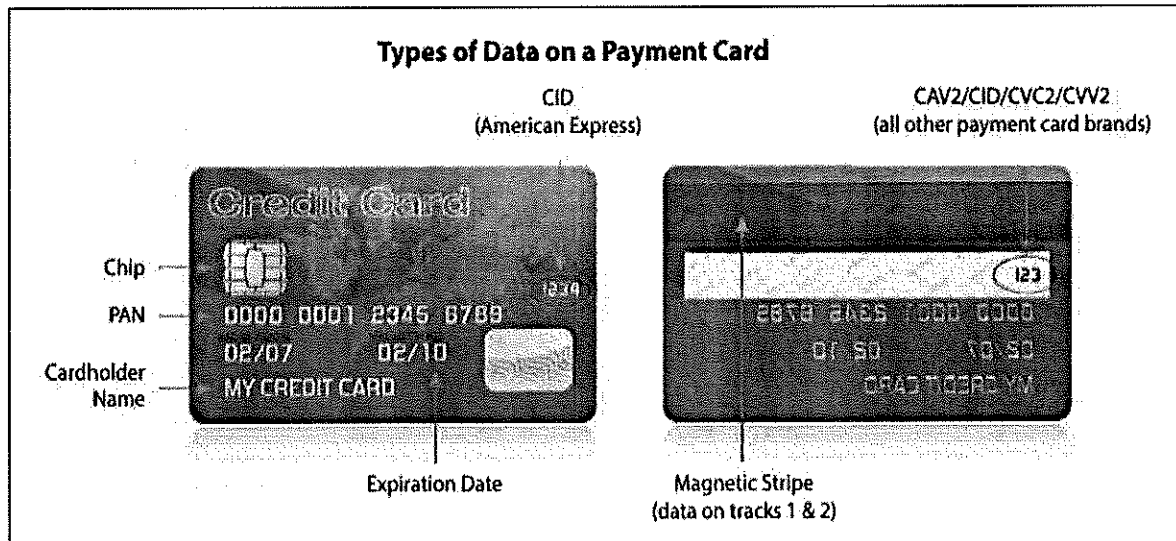
16. A large portion of WaWa's sales are made to customers who use credit or debit cards. When a customer uses a credit or debit card, the transaction involves four primary parties: (1) the "merchant" (e.g., WaWa) where the purchase is made; (2) an "acquiring bank" (which typically is a financial institution that contracts with the merchant to process its payment card transactions); (3) a "card network" or "payment processor" (such as Visa and MasterCard); and (4) the "issuer" (which is a financial institution that issues credit and debit cards to its customers).

17. Processing a payment card transaction involves four major steps:

- *Authorization* – when a customer presents a card to make a purchase, WaWa requests authorization of the transaction from the card's issuer;

- *Clearance* – if the issuer authorizes the transaction, WaWa completes the sale to the customer and forwards a purchase receipt to the acquiring bank with which it has contracted;
- *Settlement* – the acquiring bank pays WaWa for the purchase and forwards the receipt to the issuer, which then reimburses the acquiring bank; and
- *Post-Settlement* – the issuer posts the charge to the customer's credit or debit account.

18. In processing payment card transactions, merchants acquire a substantial amount of information about each customer, including his or her full name; credit or debit card account number; card security code (the value printed on the card or contained in the microprocessor chip or magnetic strip of a card and used to validate card information during the authorization process); the card's expiration date and verification value; and the PIN number for debit cards.⁴



⁴ See PCI Security Standards Council, *PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1*, 11, July 2018, https://www.pcisecuritystandards.org/documents/PCI_DSS-ORG-v3_2_1.pdf (last accessed Dec. 22, 2019).

19. Merchants typically store this information on their computer systems and transmit it to third parties to complete the transaction. At other times, and for other reasons, merchants may also collect other personally identifiable information about their customers, including, but not limited to, financial data, mailing addresses, phone numbers, driver's license numbers, and email addresses.

20. For years, WaWa has stored in its computer systems massive amounts of customer Payment Card Data. WaWa uses this information to process payment card transactions in connection with sales to its customers. Customer Payment Card Data is an asset of considerable value to both WaWa and to hackers, who can easily sell this data, as a result of the "proliferation of open and anonymous cybercrime forums on the Dark Web that serve as a bustling marketplace for such commerce."⁵

21. WaWa is—and at all relevant times has been—aware that the Payment Card Data it maintains is highly sensitive and could be used for nefarious purposes by third parties, such as perpetrating identity theft and making fraudulent purchases. To this end, WaWa posted a job opening on or about December 4, 2019—just days before allegedly discovering the WaWa Data Breach—seeking an Information Security Incident Response Junior Analyst to "follow the processes and procedures necessary for the detection, response and remediation of cyber related attacks on the Wawa enterprise."⁶

⁵ *The Value of a Hacked Company*, KREBS ON SECURITY (July 14, 2016), <http://krebsonsecurity.com/2016/07/the-value-of-a-hacked-company/> (last accessed Dec. 23, 2019).

⁶ Indeed, WaWa Information Security Incident Response Junior Analyst, <https://www.indeed.com/viewjob?jk=7a1f2ac3eeb48eea&tk=ldsibai40p2p0800&from=serp&vjs=3> (posted Dec. 3, 2019) (last accessed Dec. 23, 2019).

22. WaWa also is—and at all relevant times has been—aware of the importance of safeguarding its customers’ Payment Card Data and of the foreseeable consequences that would occur if its data security systems were breached, specifically including the fraud losses and theft that would be imposed on consumers, such as Plaintiff. Indeed, WaWa’s December 4, 2019 job posting also requires the successful applicant have a “[v]ery basic understanding of relevant legal and regulatory requirements, such as: Payment Card Industry Data Security Standard.” *Id.*

23. In addition to its general duty to act reasonably in handling and safeguarding customers’ Payment Card Data to prevent the risk of foreseeable harm to others, WaWa is—and at all relevant times has been—obligated to safeguard such information by, among other things, industry standards, federal law, and its own commitments, internal policies, and procedures.

B. The WaWa Data Breach: March 2019 to Present

24. Beginning as early as March 2019, computer hackers took advantage of vulnerabilities in WaWa’s computer and point-of-sale systems to install malware that ultimately infected potentially every WaWa location in the United States. Through this malware, the hackers were able to steal WaWa’s customers’ Payment Card Data that WaWa had collected in conjunction with its customers’ purchases.

25. On December 19, 2019 (approximately ten months after hackers first installed malware on its computer processors), WaWa announced that it was investigating a theft its customers’ Payment Card Data. WaWa explained, “malware affected payment card information, including credit and debit card numbers, expiration dates, and cardholder names on payment

cards used at potentially all Wawa in-store payment terminals and fuel dispensers beginning at different points in time after March 4, 2019 and ending on December 12, 2019.”⁷

26. Taking advantage of WaWa’s lax data security and delay in discovering the malware on its servers, hackers were able to gather large amounts of Payment Card Data. With that Payment Card Data, unknown perpetrators are now capable of making undetected fraudulent purchases on credit and debit cards belonging to Plaintiff and members of the Class. Unknown perpetrators are also capable of specifically targeting and draining debit accounts with large amounts of money in them belonging to Plaintiff and members of the Class. By failing to timely identify that its systems had been subjected to a data breach, WaWa allowed hackers to have unfettered access to WaWa’s computer and point-of-sale systems to obtain customers’ Payment Card Data for at least ten months, thereby exponentially increasing the harm suffered by Plaintiff and members of the Class.

27. Up to, and including, the period during which the WaWa data breach occurred, WaWa’s data security systems suffered from many deficiencies that made them susceptible to hackers, including, without limitation, the following:

- a. WaWa’s IT management were unqualified and failed to maintain a system of accountability over data security, thereby knowingly allowing data security deficiencies to persist;
- b. WaWa ignored well-known warnings that its point-of-sale system was susceptible to data breach;

⁷ Wawa, WaWa Data Security – Updates & Customer Resources, <https://www.wawa.com/alerts/data-security> (Dec. 19, 2019) (last accessed Dec. 23, 2019).

- c. WaWa failed to implement certain protocols that would have prevented unauthorized programs, such as malware, from being installed on its point-of-sale and other systems that accessed Payment Card Data and otherwise would have protected Payment Card Data; and
- d. WaWa failed to install software to adequately track access to its network, monitor the network for unusual activity, and prevent exfiltration of data, which would have detected the presence of hackers and prevented Payment Card Data from being stolen.

28. Attempting to downplay the seriousness of the data breach, WaWa assured its customers that “anyone impacted [] will not be responsible for fraudulent charges related to this incident.”⁸ In a separate letter to customers, WaWa’s CEO, Chris Gheysens wrote, “I want to reassure you that you will not be responsible for any fraudulent charges on your payment cards related to this incident[.]”⁹ WaWa’s assurances do not make Plaintiff and the Class members whole for the injuries they have suffered as a result of the WaWa Data Breach.

C. WaWa Failed to Comply with Its Duties

1. WaWa Failed to Comply with Industry Standards for Data Security

29. WaWa failed to comply with industry standards for data security and actively mishandled the data entrusted to it by its customers.

30. The Payment Card Industry Security Standards Council promulgates minimum standards, which apply to all organizations that store, process, or transmit Payment Card Data.

⁸ Wawa, WaWa Notifies Customers of Data Security Incident, https://s3.amazonaws.com/wawa-kentico-prod/wawa/media/misc/wawa-data-security-incident-wire-release-12_19_2019.pdf (Dec. 19, 2019) (last accessed Dec. 23, 2019).

⁹ Wawa, An Open Letter from WaWa CEO Chris Gheysens to Our Customers, <https://www.wawa.com/alerts/data-security> (Dec. 19, 2019) (last accessed Dec. 23, 2019).

These standards are known as the Payment Card Industry Data Security Standard (“PCI DSS”). PCI DSS is the industry standard governing the security of Payment Card Data, although it sets the minimum level of what must be done, not the maximum.

31. PCI DSS version 3.2.1, released in May 2018 and in effect at the time of the WaWa Data Breach, imposes the following 12 “high-level” mandates:¹⁰

The PCI Data Security Standard	
PCI DSS is the global data security standard adopted by the payment card brands for all entities that process, store or transmit cardholder data and/or sensitive authentication data. It consists of steps that mirror security best practices.	
Goals	PCI DSS Requirements
Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel

¹⁰ PCI Security Standards Council, *PCI DSS Quick Reference Guide: Understanding the Payment Card Industry Data Security Standard version 3.2.1*, 9, July 2018, https://www.pcisecuritystandards.org/documents/PCI_DSS-ORG-v3_2_1.pdf (last accessed Dec. 22, 2019).

32. Furthermore, PCI DSS 3.2.1 set forth detailed and comprehensive requirements that had to be followed to meet each of the 12 mandates.

33. Among other things, PCI DSS 3.2.1 requires WaWa to properly secure Payment Card Data; not store cardholder data beyond the time necessary to authorize a transaction; to timely upgrade its point-of-sale software; implement proper network segmentation; encrypt Payment Card Data at the point-of-sale; restrict access to Payment Card Data to those with a need to know; and establish a process to identify; and timely fix security vulnerabilities. Upon information and belief, WaWa failed to comply with each of these requirements.

2. WaWa Failed to Comply with Federal Trade Commission Requirements

34. According to the Federal Trade Commission (“FTC”), the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by §5 of the Federal Trade Commission Act of 1914 (“FTC Act”), 15 U.S.C. §45.

35. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network’s vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

36. The FTC has also published a document entitled “FTC Facts for Business,” which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.

37. The FTC has issued orders against businesses that failed to employ reasonable measures to secure Payment Card Data. These orders provide further guidance to businesses in regard to their data security obligations.

38. In the years leading up to the WaWa data breach, and during the course of the breach itself, WaWa failed to follow the guidelines set forth by the FTC and actively mishandled the management of its IT security. Furthermore, by failing to have reasonable data security measures in place, WaWa engaged in an unfair act or practice within the meaning of §5 of the FTC Act.

3. PLAINTIFF’S TRANSACTIONS

39. WaWa failed to protect its customers’ Payment Card Data and as a result, Plaintiff and Class members have and will suffer various injuries.

40. On November 13, 2019, Plaintiff purchased gas at a WaWa in Feasterville, Pennsylvania using a debit card issued to her by her credit union. Plaintiff returned to this WaWa location two weeks later, on November 27, 2019, to purchase gas. She used the same debit card to complete this purchase. These were the only times that Plaintiff has ever shopped at the WaWa in Feasterville, Pennsylvania.

41. WaWa confirmed that the location Plaintiff visited was potentially affected by the WaWa Data Breach.¹¹

¹¹ Wawa, An Open Letter from WaWa CEO Chris Gheysens to Our Customers, <https://www.wawa.com/alerts/data-security> (Dec. 19, 2019) (“This malware affected customer

42. To prepare for Black Friday shopping the next day, Plaintiff logged into and reviewed her credit union checking account on Thanksgiving Day, November 28, 2019. At that time, Plaintiff discovered that an unknown third party had accessed and drained her checking account of hundreds of dollars, leaving Plaintiff with a negative balance on the eve of the holiday shopping season.

43. Specifically, on November 26, 2019—less than two weeks after buying gas at the WaWa in Feasterville, Pennsylvania for the first time—a \$125.00 withdrawal was made from Plaintiff's checking account using Plaintiff's debit card. The withdrawal was made at a Shell Oil in Lantana, Florida. Plaintiff did not make this withdrawal.

44. Similarly, on November 28, 2019—the day after Plaintiff's second purchase at the WaWa in Feasterville, Pennsylvania—a second \$125.00 withdrawal was made from Plaintiff's checking account using Plaintiff's debit card. It too was made at a Shell Oil in Lantana, Florida. Plaintiff did not make this second withdrawal.

45. To protect against additional theft, Plaintiff immediately froze her account on Thursday, November 28, 2019.

46. By freezing her account, Plaintiff could not access the additional funds her employer deposited into it on Friday, November 29, 2019.

47. Because her credit union was closed on Thanksgiving Day, the Friday after it, and that weekend, Plaintiff could not contact a member representative until Monday, December 2, 2019—five days after discovering the fraudulent charges to her account.

payment card information used at potentially all Wawa locations beginning at different points in time after March 4, 2019 and until it was contained.”) (last accessed Dec. 23, 2019).

48. When she finally reached her credit union on Monday, December 2, 2019, Plaintiff cancelled her debit card and ordered a replacement. Plaintiff received her replacement debit card approximately ten days later, on or about December 12, 2019.

49. Plaintiff spent Thanksgiving and the shopping days after it monitoring her online checking account, contacting her credit union, freezing her account altogether, and generally spending time and losing productivity and enjoyment from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the theft. Because the theft left her account with a negative balance, Plaintiff also lost opportunities to purchase gifts at discounted prices during the 2019 holiday shopping season.

50. Plaintiff would not have used her debit card to make purchases at WaWa had WaWa told her that it lacked adequate computer systems and data security practices to safeguard customers' Payment Card Data from theft. Indeed, Plaintiff would not have shopped at WaWa at all during the period of the WaWa Data Breach and, thus, she suffered actual injury and damages in paying money to WaWa for the purchase of products from WaWa that she would not have paid had WaWa made such disclosure.

51. Plaintiff also suffered actual injury in the form of damages to and diminution in the value of her Payment Card Data—a form of intangible property that Plaintiff entrusted to WaWa for the purpose of purchasing its products and that was compromised in and as a result of the WaWa Data Breach.

52. Additionally, Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by their Payment Card Data being placed in the hands of criminals who have already misused such information, as evidenced by the compromise of Plaintiffs' payment cards.

53. Moreover, Plaintiff has a continuing interest in ensuring that her private information, which remains in WaWa's possession, is protected and safeguarded from future breaches.

V. CLASS ACTION ALLEGATIONS

54. Plaintiff brings this action on behalf of itself and as a class action, pursuant to the provisions of Rules 23(a), 23(b)(2), and 23(b)(3) of the Federal Rules of Civil Procedure, on behalf of the following class (the "Class"):

All persons in the United States who made a credit or debit card purchase at any affected WaWa location from March 4, 2019 to the present.

55. Excluded from the Class are Defendants and their subsidiaries and affiliates; all employees of Defendants; all persons who make a timely election to be excluded from the Class; government entities; and the judge to whom this case is assigned, including his/her immediate family and court staff.

56. Certification of Plaintiff's claims for Class-wide treatment is appropriate because all elements of Fed. R. Civ. P. 23(a), (b)(2)-(3) are satisfied. Plaintiff can prove the elements of its claims on a Class-wide basis using the same evidence as would be used to prove those elements in an individual action alleging the same claims.

57. **Numerosity:** All requirements of Fed. R. Civ. P. 23(a)(1) are satisfied. The members of the Class are so numerous and geographically dispersed that individual joinder of all Class members is impracticable. While Plaintiff is informed and believes that there are thousands of members of the Class, the precise number of Class members is unknown to Plaintiff. Class members may be identified through objective means. Class members may be notified of the

pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, Internet postings, and/or published notice.

58. **Commonality and Predominance:** All requirements of Fed. R. Civ. P. 23(a)(2) and 23(b)(3) are satisfied. This action involves common questions of law and fact, which predominate over any questions affecting individual Class members, including, without limitation:

- a. whether Defendants engaged in the active misfeasance and misconduct alleged herein;
- b. whether WaWa owed a duty to Plaintiff and members of the Class to act reasonably to protect Payment Card Data;
- c. whether WaWa failed to provide adequate security to protect Payment Card Data;
- d. whether WaWa negligently, or otherwise improperly, allowed third parties to access Payment Card Data;
- e. whether Plaintiff and members of the Class were injured and suffered damages and ascertainable losses;
- f. whether WaWa's failure to provide adequate security proximately caused Plaintiff's and Class members' injuries;
- g. whether Plaintiff and members of the Class are entitled to damages and, if so, the measure of such damages; and
- h. whether Plaintiff and members of the Class are entitled to declaratory and injunctive relief.

59. **Typicality:** All requirements of Fed. R. Civ. P. 23(a)(3) are satisfied. Plaintiff is a member of the Class, having used her payment card at an affected WaWa location and had her Payment Card Data compromised in the WaWa data breach. Plaintiff's claims are typical of the other Class members' claims because, among other things, all Class members were comparably injured through Defendants' conduct.

60. **Adequacy of Representation:** All requirements of Fed. R. Civ. P. 23(a)(4) are satisfied. Plaintiff is an adequate Class representative because she is a member of the Class and her interests do not conflict with the interests of the other members of the Class that she seeks to represent. Plaintiff is committed to pursuing this matter for the Class with the Class's collective best interests in mind. Plaintiff has retained counsel competent and experienced in complex class action litigation of this type and Plaintiff intends to prosecute this action vigorously. Plaintiff, and her counsel, will fairly and adequately protect the Class's interests.

61. **Predominance and Superiority:** All requirements of Fed. R. Civ. P. 23(b)(3) are satisfied. As described above, common issues of law or fact predominate over individual issues. Resolution of those common issues in Plaintiff's individual case will also resolve them for the Class's claims. In addition, a class action is superior to any other available means for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiff and the other Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Defendants, so it would be impracticable for members of the Class to individually seek redress for Defendants' wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and

increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single court.

62. **Cohesiveness:** All requirements of Fed. R. Civ. P. 23(b)(2) are satisfied. Defendants have acted, or refused to act, on grounds generally applicable to the Class making final declaratory or injunctive relief appropriate.

VI. CHOICE OF LAW

63. WaWa's acts and omissions discussed herein were orchestrated and implemented at its corporate headquarters in Pennsylvania and the tortious and deceptive acts complained of occurred in, and radiated from, Pennsylvania.

64. The key wrongdoing at issue in this litigation (WaWa's failure to employ adequate data security measures) emanated from WaWa's headquarters in Pennsylvania.

65. Upon information and belief, WaWa's point-of-sale system and IT personnel operate out of and are located at WaWa's headquarters in Pennsylvania. To this end, WaWa currently is hiring an Information Security Incident Response Junior Analyst based in WaWa, Pennsylvania, to "follow the processes and procedures necessary for the detection, response and remediation of cyber related attacks on the Wawa enterprise."¹²

66. Pennsylvania, which seeks to protect the rights and interests of Pennsylvania and other U.S. businesses against a company doing business in Pennsylvania, has a greater interest in the claims of Plaintiff and the Class members than any other state and is most intimately concerned with the outcome of this litigation.

¹² Indeed, WaWa Information Security Incident Response Junior Analyst, <https://www.indeed.com/viewjob?jk=7a1f2ac3eeb48eea&tk=1dsibai40p2p0800&from=serp&vis=3> (posted Dec. 3, 2019) (last accessed Dec. 22, 2019).

67. Application of Pennsylvania law to a nationwide Class with respect to Plaintiff's and the Class members' claims is neither arbitrary nor fundamentally unfair because Pennsylvania has significant contacts and a significant aggregation of contacts that create a state interest in the claims of Plaintiff and the nationwide Class.

68. The location where Plaintiff and Class members' were injured was fortuitous and WaWa could not have foreseen where the injury would take place, as WaWa didn't know which banks WaWa's customers used and the location of these banks' headquarters, or principal places of business, at the time of the breach.

VII. CAUSES OF ACTION

COUNT I

Negligence

On behalf of the Plaintiff and the Class

69. Plaintiff incorporates by reference all preceding allegations, as though fully set forth herein.

70. WaWa owed—and continues to owe—a duty to Plaintiff and the Class to use reasonable care in safeguarding Payment Card Data and to discover any breach in a timely manner, so that compromised financial accounts and credit cards can be closed quickly in order to avoid fraudulent transactions. This duty arises from several sources, including, but not limited to, the sources described below, and is independent of any duty WaWa owed as a result of its contractual obligations.

71. WaWa has a common law duty to prevent the foreseeable risk of harm to others, including Plaintiff and the Class. It was certainly foreseeable to WaWa that injury would result from a failure to use reasonable measures to protect Payment Card Data and to detect breaches in a timely manner. It was also foreseeable that, if reasonable security measures were not taken, hackers would steal Payment Card Data belonging to millions of WaWa's customers; thieves

would use Payment Card Data to make large numbers of fraudulent transactions; and that the resulting financial losses would be immense.

72. WaWa assumed the duty to use reasonable security measures as a result of its conduct.

73. In addition to its general duty to exercise reasonable care, WaWa also had a duty of care as a result of the special relationship that existed between WaWa and Plaintiff and members of the Class. The special relationship arose because customers entrusted WaWa with their Payment Card Data. Only WaWa was in a position to ensure that its systems were sufficient to protect against the harm to its customers from a data breach.

74. WaWa's duty to use reasonable data security measures also arose under §5 of the FTC Act, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect Payment Card Data by businesses such as WaWa. The FTC publications and data security breach orders described above further form the basis of WaWa's duty. In addition, individual states have enacted statutes based upon the FTC Act that also create a duty on the part of WaWa.

75. WaWa's duty to use reasonable care in protecting Payment Card Data arose not only as a result of the common law and the statutes described above, but also because it was bound by, and had committed to comply with, industry standards, specifically including PCI DSS.

76. WaWa breached its common law, statutory, and other duties and thus, was negligent by failing to use reasonable measures to protect Plaintiff's Payment Card Data from the hackers who perpetrated the data breach and by failing to discover the breach timely. Upon

information and belief, the specific negligent acts and omissions committed by WaWa include, but are not limited to, some, or all, of the following:

- a. failure to delete cardholder information after the time period necessary to authorize the transaction;
- b. failure to employ systems to protect against malware;
- c. failure to comply with industry standards for software and point-of-sale security;
- d. failure to track and monitor access to its network and cardholder data;
- e. failure to limit access to those with a valid purpose;
- f. failure to adequately staff and fund its data security operation;
- g. failure to use due care in hiring, promoting, and supervising those responsible for its data security operations; and
- h. failure to recognize that hackers were stealing Payment Card Data from its network while the data breach was taking place.

77. In connection with the conduct described above, WaWa acted wantonly, recklessly, and with complete disregard for the consequences.

78. As a direct and proximate result of WaWa's negligence, Plaintiff and members of the Class have and will suffer actual losses and damages as described above.

COUNT II
Negligence *Per Se*
On behalf the Plaintiff and the Class

79. Plaintiff incorporates by reference all preceding allegations as though fully set forth herein.

80. Section 5 of the FTC Act prohibits “unfair . . . practices in or affecting commerce,” including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as WaWa, of failing to use reasonable measures to protect Payment Card Data. The FTC publications and orders described above also form part of the basis of WaWa’s duty.

81. WaWa violated §5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Payment Card Data and not complying with applicable industry standards, including PCI DSS, as described in detail herein. WaWa’s conduct was particularly unreasonable given the nature and amount of Payment Card Data it obtained and stored and the foreseeable consequences of a data breach at one of the country’s largest private companies, including, specifically, the immense damages that would result to consumers and financial institutions.

82. WaWa’s violation of §5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

83. Plaintiff and members of the Class are within the class of persons that §5 of the FTC Act (and similar state statutes) was intended to protect.

84. The harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over 50 enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiff and the Class.

85. As a direct and proximate result of WaWa’s negligence, Plaintiff and members of the Class have and will suffer actual losses and damages as described above.

COUNT III
Unjust Enrichment
On behalf the Plaintiff and the Class

86. Plaintiff incorporates by reference all preceding allegations, as though fully set forth herein.

87. Plaintiff and Class members conferred a monetary benefit on WaWa. Specifically, they purchased goods and services from WaWa and provided WaWa with their payment information. In exchange, Plaintiff and Class members should have received from WaWa the goods and services that were the subject of the transaction and should have been entitled to have WaWa protect their Payment Card Data with adequate data security.

88. WaWa knew that Plaintiff and Class members conferred a benefit on WaWa and accepted and has accepted or retained that benefit. WaWa profited from the purchases and used the Payment Card Data of Plaintiff and Class members for business purposes.

89. WaWa failed to secure the Payment Card Data of Plaintiff and Class members and, therefore, did not provide full compensation for the benefit the Plaintiff and Class members provided.

90. WaWa acquired the Payment Card Data through inequitable means it failed to disclose the inadequate security practices previously alleged.

91. If Plaintiff and Class members knew that WaWa would not secure their Payment Card Data using adequate security, they would not have made purchases at WaWa's convenience stores.

92. Plaintiff and Class members have no adequate remedy at law.

93. Under the circumstances, it would be unjust for WaWa to be permitted to retain any of the benefits that Plaintiff and Class members conferred on it.

94. WaWa should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class members, proceeds that it unjustly received from them. In the alternative, WaWa should be compelled to refund the amounts that Plaintiff and Class members overpaid.

COUNT IV
Declaratory and Injunctive Relief
On behalf of Plaintiff and the Class

95. Plaintiff incorporates by reference all preceding allegations, as though fully set forth herein.

96. Under the Declaratory Judgment Act, 28 U.S.C. §§2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, which are tortious and which violate the terms of the federal and state statutes described herein.

97. An actual controversy has arisen in the wake of WaWa's data breach regarding its common law and other duties to reasonably safeguard Payment Card Data. Plaintiff alleges that WaWa's data security measures were inadequate and remain inadequate.

98. WaWa still possesses Payment Card Data pertaining to Plaintiff and Class members.

99. WaWa has made no announcement or notification that it has remedied the vulnerabilities in its computer data systems, and, most importantly, its POS systems and fueling stations.

100. Accordingly, WaWa has not satisfied its legal duties to Plaintiff and Class members. In fact, now that WaWa's lax approach towards data security has become public, the Payment Card Data in its possession is more vulnerable than previously.

101. Actual harm has arisen in the wake of the WaWa Data Breach regarding WaWa's duties of care to provide data security measures to Plaintiffs and Class members.

102. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. WaWa continues to owe a legal duty to secure its customers' personal and financial information—specifically including information pertaining to credit and debit cards used by WaWa's customers—and to notify financial institutions of a data breach under the common law, §5 of the FTC Act, PCI DSS standards, its commitments, and various state statutes;
- b. WaWa continues to breach this legal duty by failing to employ reasonable measures to secure its customers' personal and financial information; and
- c. WaWa's ongoing breaches of its legal duty continue to cause Plaintiff harm.

103. The Court also should issue corresponding injunctive relief requiring WaWa to employ adequate security protocols, consistent with industry standards, to protect its Payment Card Data. Specifically, this injunction should, among other things, direct WaWa to:

- a. utilize industry standard encryption to encrypt the transmission of cardholder data at the point-of-sale and at all other times;
- b. implement encryption keys in accordance with industry standards;
- c. implement EMV technology;
- d. engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

- e. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;
- f. regularly test its systems for security vulnerabilities, consistent with industry standards;
- g. comply with all PCI DSS standards pertaining to the security of its customers' personal and confidential information; and
- h. install all upgrades recommended by manufacturers of security software and firewalls used by WaWa.

104. If an injunction is not issued, Plaintiff will suffer irreparable injury and lack an adequate legal remedy in the event of another data breach at WaWa. The risk of another such breach is real, immediate, and substantial. If another breach at WaWa occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct. Simply put, monetary damages, while warranted to compensate Plaintiff and the Class for out of pocket damages that are legally quantifiable and provable, do not cover the full extent of injuries suffered by Plaintiff and the Class, which include monetary damages that are not legally quantifiable or provable.

105. The hardship to Plaintiff and the Class, if an injunction is not issued, exceeds the hardship to WaWa, if an injunction is issued. Among other things, if another massive data breach occurs at WaWa, Plaintiff and members of the Class will likely incur hundreds of millions of dollars in damage. On the other hand, the cost to WaWa of complying with an injunction by employing reasonable data security measures is relatively minimal and WaWa has a pre-existing legal obligation to employ such measures.

106. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at WaWa, thus eliminating the injuries that would result to Plaintiff, the Class, and the millions of consumers whose confidential information would be compromised.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the Class, respectfully requests that the Court:

- A. Certify the Class and appoint Plaintiff and Plaintiff's counsel to represent the Class;
- B. Enter a monetary judgment in favor of Plaintiff and members of the Class to compensate them for the injuries suffered, together with pre-judgment and post-judgment interest, treble damages, and penalties where appropriate;
- C. Enter a declaratory judgment in favor of Plaintiff and the Class, as described above;
- D. Grant Plaintiff the injunctive relief requested;
- E. Award Plaintiff and the Class reasonable attorneys' fees and costs of suit, as allowed by law; and
- F. Award such other and further relief as this Court may deem just and proper.

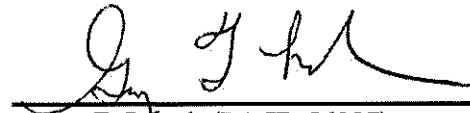
DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury of any and all issues in this action so triable.

Dated: December 23, 2019

Respectfully submitted,

CARLSON LYNCH, LLP

A handwritten signature in black ink, appearing to read "G. F. Lynch", is written over a horizontal line.

Gary F. Lynch (PA ID 56887)

Jamisen A. Etzel (PA ID 311554)

Kevin W. Tucker (PA ID 312144)

1133 Penn Avenue, 5th Floor

Pittsburgh, PA 15222

Tel. (412) 322-9243

glynch@carlsonlynch.com

jetzel@carlsonlynch.com

ktucker@carlsonlynch.com

Counsel for Plaintiff